DoD Privacy Impact Assessment (PIA)

1. Department of Defense (DoD) Component.

United States Air Force (USAF)

2. Name of Information Technology (IT) System.

Armed Forces Entertainment Information System (AFEIS)

3. Budget System Identification Number (SNAP-IT Initiative Number).

3085

4. System Identification Number(s) (IT Registry/Defense IT Portfolio Repository (DITPR)).

9622

5. IT Investment (Office of Management and Budget (OMB) Circular A-11) Unique Identifier (if applicable).

007-57-01-34-01-3085-00

6. Privacy Act System of Records Notice (SORN) Identifier (if applicable).

A SORN is expected to be published in the Federal Register by 2009.

7. OMB Information Collection Requirement Number (if applicable) and Expiration Date.

Not Applicable.

8. Type of authority to collect information (statutory or otherwise).

Executive Order (EO) 9397 (Social Security Number - SSN)
10 United States Code (U.S.C.) 8013, Secretary of the Air Force
Department of Defense Instruction (DoDI) 1330.13, Armed Forces Entertainment Program
Air Force Instruction (AFI) 34-126(I), Armed Forces Entertainment Program

9. Provide a brief summary or overview of the IT system (activity/purpose, present lifecycle phase, system owner, system boundaries and interconnections, location of system and components, and system backup).

The system assists the Armed Forces Entertainment (AFE) division in administering the Armed Forces Entertainment program. The system contains modules for recording tour information (including the entertainers on the tour), generating appropriate documents (such as travel orders), and financial documents such as proposals, contracts, expense forms, and summary cost data. The system is capable of generating travel itineraries as well. Present lifecycle phase is sustainment. AFEIS does not talk to other systems. Backups are maintained. The system owner is AFE, Arlington, Virginia.

10. Describe what information in identifiable form will be collected and the nature and source of the information (e.g., names, Social Security Numbers, gender, race, other component IT systems, IT systems from agencies outside Department of Defense (DoD), etc.).

All data in the AFEIS database is entered by authorized AFEIS users. Personal data include:

- The names, SSNs, and passport numbers of entertainers
- The names, business telephone numbers, fax numbers, Defense Switched Network (DSN) telephone numbers, email addresses, service affiliations, ranks, and grades of authorized system users.

11. Describe how the information will be collected (e.g., via the Web, via paper-based collection, etc.).

Authorized users will enter data via the web from information provided by the entertainers in paper form.

12. Describe the requirement and why the information in identifiable form is to be collected (e.g., to discharge a statutory mandate, to execute a Component program, etc.).

AFE operates the Armed Forces Entertainment Program under guidance from DoDI 1330.13 and AFI 34-126. AFEIS assists AFE in administering the tours put on by the Armed Services Entertainment program. It has provisions for identifying the performers for each tour, tracking tour itineraries, recording tour expenses, generating standard documents such as travel orders, and calculating the honoraria for the entertainers.

13. Describe how the information in identifiable form will be used (e.g., to verify existing data, etc.).

The information in the system will be used to schedule tours; assign entertainers; schedule itineraries; capture tour expenses; and to generate travel orders, immunization requirements letters, entertainment contracts, financial documents (such as contracts with the performers and payment forms), travel requests, and releases.

14. Describe whether the system derives or creates new data about individuals through aggregation.

The system does not derive or create new data about individuals through aggregation.

15. Describe with whom the information in identifiable form will be shared, both within the Component and outside the Component (e.g., other DoD Components, Federal agencies, etc.).

Information may be disclosed to agencies for the Department of Defense, Reserve Components, National Guard, and other federal agencies. There is no disclosure outside the Federal Government.

Personal data could be released without the employee's consent for the "Blanket Routine Uses" in accordance with the provisions of AFI 33-332, Privacy Act Program, Chapter 12, Paragraph 4, Rules for Releasing Privacy Act Information Without Consent of the Subject.

16. Describe any opportunities individuals will have to object to the collection of information in identifiable form about themselves or to consent to the specific uses of the information in identifiable form. Where consent is to be obtained, describe the process regarding how the individual is to grant consent.

Individuals are shown a Privacy Act Statement (PAS). Presumably, an entertainer who does not wish to have her or his SSN and passport number in the system does not have to work for the Armed Services. If anyone is concerned about personal information in this system, he or she would contact the system owner.

17. Describe any information that is provided to an individual, and the format of such information (Privacy Act Statement, Privacy Advisory) as well as the means of delivery (e.g., written, electronic, etc.), regarding the determination to collect the information in identifiable form.

Individuals are shown a PAS.

Appearing on every web page is a link to a notice reminding system users of the government's obligations to protect personal data and use it only for authorized purposes.

18. Describe the administrative/business, physical, and technical processes and controls adopted to secure, protect, and preserve the confidentiality of the information in identifiable form.

18.1. The PIA is based on proper implementation, validation, and verification of the baseline information assurance controls for CONFIDENTIALITY in accordance with Department of Defense Instruction (DoDI) 8500.2, *Information Assurance (IA) Implementation.* The controls address the administrative, physical, and technical controls

required to secure, protect, and preserve the confidentiality of information in identifiable form.

18.2. AFEIS is a mission assurance category (MAC) III system with a confidentiality level of "Sensitive." AFEIS is not fully certified and accredited but is in phase III of the Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) and has implemented/validated the DoDI 8500.2 baseline controls for systems with a confidentiality level of "**SENSITIVE."**

Baseline IA controls validated for AFEIS:

EBBD-2	Boundary Defense
EBPW-1	Public Wide Area Network Connection
EBRP-1	Remote Access for Privileged Functions
EBRU-1	Remote Access for User Functions
ECAD-1	Affiliation Display
ECAR-2	Audit Record Content – Sensitive Systems
ECAT-1	Audit Trail, Monitoring, Analysis, and Reporting
ECCR-1	Encryption for Confidentiality (Data at Rest)
ECCT-1	Encryption for Confidentiality (Data at Transmit)
ECIC-1	Interconnections among DoD Systems and Enclaves
ECLO-1	Logon
ECLP-1	Least Privilege
ECML-1	Marking and Labeling
ECMT-1	Conformance Monitoring and Testing
ECNK-1	Encryption for Need-to-Know
ECRC-1	Resource Control
ECRR-1	Audit Record Retention
ECTC-1	Tempest Controls
ECWM-1	Warning Message
IAAC-1	Account Control
IAGA-1	Group Identification and Authentication
IAIA-1	Individual Identification and Authentication
PRAS-1	Access to Information
PRMP-1	Maintenance Personnel
PRNK-1	Access to Need-to-Know Information
PRTN-1	Information Assurance Training
PECF-1	Access to Computing Facilities
PECS-1	Clearing and Sanitizing
PEDI-1	Data Interception
PEPF-1	Physical Protection of Facilities
PEPS-1	Physical Security Testing
PESP-1	Workplace Security Procedures
PESS-1	Storage
PEVC-1	Visitor Control to Computing Facilities
DCAS-1	Acquisition Standards

DCSR-2 Specified Robustness – Medium

SORN Review: A SORN is expected to be published in the Federal Register by 2009.

19. Identify whether the IT system or collection of information will require a System of Records notice as defined by the Privacy Act of 1974 and as implemented by DoD Directive 5400.11, DoD Privacy Program, May 8, 2007; and DoD 5400.11-R, Department of Defense Privacy Program, May 14, 2007. If so, and a System Notice has been published in the Federal Register, the Privacy Act System of Records Identifier must be listed in question 6 above. If not yet published, state when publication of the Notice will occur.

A SORN is expected to be published in the Federal Register by 2009.

20. Describe/evaluate any potential privacy risks regarding the collection, use, and sharing of the information in identifiable form. Describe/evaluate any privacy risks in providing individuals an opportunity to object/consent or in notifying individuals. Describe/evaluate further any risks posed by the adopted security measures.

Only authorized users can access the data in the system. They must provide their usernames and passwords to access the system.

Since it is not possible to search directly for private data by name or personal identifier (one can only reach it by searching for a specific tour, identifying the entertainers assigned to that tour, and looking in the financial data for that tour), the risk that a careless or dishonest government employee would be indiscreet is considered minimal.

21. State classification of information/system and whether the PIA should be published or not. If not, provide rationale. If a PIA is planned for publication, state whether it will be published in full or summary form.

Unclassified. This PIA will be published in full.

Privacy Impact Assessment Approval Page for Armed Forces Entertainment Information System (AFEIS)

Privacy Impact Assessment Approval Page for AFEIS

Preparing Official [redacted] (Signature) 6 Aug 08 (Date)
Name: [redacted]
Title: Chief, Armed Forces Entertainment
Organization: AF/AIST
Work Telephone Number: [redacted]
E-mail: [redacted]

Information Assurance Official [redacted] (Signature) 13 AUG 08 (Date)
Name: [redacted]
Title: Systems Planning and Integration
Organization: AF/A1XI
Work Telephone Number: [redacted]
E-mail: [redacted]

HQ Air Force Privacy Act Officer [redacted] ~~(Date)~~ 13 Aug 08
Name: [redacted]
Organization: HAF/IMIC
Work Telephone Number: [redacted]
E-mail: [redacted]

HQ Air Force Information Assurance Official [redacted] Signature) 22 Aug 08 (Date)
Name: [redacted]
Organization: SAF/XCPPI
Work Telephone Number: [redacted]
E-mail: [redacted]

HQ Air Force Privacy Act Officer [redacted] (Signature) 8/25/08 (Date)
Name: [redacted]
Organization: SAF/XCPPI
Work Telephone Number: [redacted]
E-mail: [redacted]

Reviewing Official [redacted] ~~(Signature)~~ 12 Sep 08 (Date)
Name: [redacted]
Title: Air Force Chief Information Officer
Organization: SAF/XC, Office of Warfighting Integration and Chief Information Officer
Work Telephone Number: [redacted]
E-mail: [redacted]

PIA for AF EIS